PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY

(Chapter II of the Patent Cooperation Treaty)

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference	FOR FURTHER ACTION	See Form PCT/IPEA/416
9869SG186/MHK/nbs		
International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/SG2004/000312	24 September 2004	26 September 2003

International Patent Classification (IPC) or national classification and IPC

Int. Cl.

G06T 1/00 (2006.01)

Applicant

AGENCY FOR SCIENCE, TECHNOLOGY AND RESEARCH et al

1. This report is the international preliminary examination report, established by this International Preliminary Examining Authority under Article 35 and transmitted to the applicant according to Article 36.
2. This REPORT consists of a total of 3 sheets, including this cover sheet.
3. This report is also accompanied by ANNEXES, comprising:
   a. [X] *(sent to the applicant and to the International Bureau)* a total of **10** sheets, as follows:
      - [X] sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications authorized by this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions).
      - [ ] sheets which supersede earlier sheets, but which this Authority considers contain an amendment that goes beyond the disclosure in the international application as filed, as indicated in item 4 of Box No. I and the Supplemental Box.

   b. [ ] *(sent to the International Bureau only)* a total of (indicate type and number of electronic carrier(s)) , containing a sequence listing and/or table related thereto, in electronic form only, as indicated in the Supplemental Box Relating to Sequence Listing (see Section 802 of the Administrative Instructions).

4. This report contains indications relating to the following items:

[X]	Box No. I	Basis of the report
[ ]	Box No. II	Priority
[ ]	Box No. III	Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
[ ]	Box No. IV	Lack of unity of invention
[X]	Box No. V	Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
[ ]	Box No. VI	Certain documents cited
[ ]	Box No. VII	Certain defects in the international application
[ ]	Box No. VIII	Certain observations on the international application

Date of submission of the demand	Date of completion of this report
29 June 2005	13 January 2006
Name and mailing address of the IPEA/AU	Authorized Officer
AUSTRALIAN PATENT OFFICE PO BOX 200, WODEN ACT 2606, AUSTRALIA E-mail address: pct@ipaustralia.gov.au Facsimile No. (02) 6285 3929	**Matthew Hollingworth** Telephone No. (02) 6283 2024

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY

International application No.
PCT/SG2004/000312

Box No. I Basis of the report

1. With regard to the language, this report is based on:

[X] The international application in the language in which it was filed

[ ] A translation of the international application into , which is the language of a translation furnished for the purposes of:

[ ] international search (under Rules 12.3(a) and 23.1 (b))

[ ] publication of the international application (under Rule 12.4(a))

[ ] international preliminary examination (Rules 55.2(a) and/or 55.3(a))

2. With regard to the elements of the international application, this report is based on *(replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report)*:

[ ] the international application as originally filed/furnished

[X] the description:

pages **1-2, 7-14** as originally filed/furnished
pages* **3-6, 20** received by this Authority on **29th June 2005** with the letter of **the same date**
pages* received by this Authority on with the letter of

[X] the claims:

pages as originally filed/furnished
pages* as amended (together with any statement) under Article 19
pages* **15-19** received by this Authority on **29th June 2005** with the letter of **the same date**
pages* received by this Authority on with the letter of

[X] the drawings:

pages **1-5** as originally filed/furnished
pages* received by this Authority on with the letter of
pages* received by this Authority on with the letter of

[ ] a sequence listing and/or any related table(s) - see Supplemental Box Relating to Sequence Listing.

3. [ ] The amendments have resulted in the cancellation of:

[ ] the description, pages
[ ] the claims, Nos.
[ ] the drawings, sheets/figs
[ ] the sequence listing *(specify)*:
[ ] any table(s) related to the sequence listing *(specify)*:

4. [ ] This report has been established as if (some of) the amendments annexed to this report and listed below had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).

[ ] the description, pages
[ ] the claims, Nos.
[ ] the drawings, sheets/figs
[ ] the sequence listing *(specify)*:
[ ] any table(s) related to the sequence listing *(specify)*:

* *If item 4 applies, some or all of those sheets may be marked "superseded."*

Box No. V **Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement**

1. Statement

Novelty (N)	Claims	1-26	YES
	Claims		NO
Inventive step (IS)	Claims		YES
	Claims	1-26	NO
Industrial applicability (IA)	Claims	1-26	YES
	Claims		NO

2. Citations and explanations (Rule 70.7)

- D1: WO 2003/030541 A2 (THE TRUSTEES OF COLUMBIA UNIVERSITY IN THE CITY OF NEW YORK), 10th April 2003

INVENTIVE STEP (IS) claim 1-26

Claims 1-26: These claims are seen to lack inventive step in light of document D1. The claims include a selectable authentication mode, a feature not disclosed in D1. However, the mere inclusion of such a mode, per se, cannot be considered to confer inventive step to the claims, since there is no characterisation in the claims of how the processing of extracted feature values is affected by which mode is selected. Since all other features of the claims are disclosed by D1, the claims lack inventive step in light of this citation.

(With reference to claim 2, it is considered that the citation's use of a user-selectable authentication bit rate constitutes the step of "selecting a desired authentication robustness level," as per claim 2, since the authentication bit rate does affect the robustness of the embedded watermark.)

SUMMARY

In accordance with a first aspect of the present invention there is provided a method of protecting a digital image, the method comprising extracting feature values from the digital image based on a selected authentication bit-rate and a selected image content; selecting an authentication mode for processing the extracted feature values, the processing of the extracted feature values comprising deriving data corresponding to the extracted feature values based on the selected authentication mode; and creating an image signature based on the data corresponding to the feature values.

The processing may comprise correcting coding (ECC) the extracted feature values to derive the data corresponding to the feature values.

The feature values from each of a plurality of codeblocks of the original digital image may be thresholded and coded to create the data corresponding to the feature values.

The processing may further comprise embedding the data corresponding to the feature values into the digital image.

The method may further comprise applying ECC coding again to parity check bits generated during the ECC coding of the extracted feature values to generate the data corresponding to the feature values.

The embedding of the data corresponding to the feature values as a watermark may be conducted in a lossy or a lossless way, based on the selected authentication mode.

The creating of the image signature may comprise applying a cryptographic hashing function to a bit sequence representing the data corresponding to the feature values.

The creating of the image signature may comprise utilising a private key.

The method may further comprise distributing the digital image, including the embedded data, as the authentic digital image.

The method may further comprise coding the digital image, including the embedded data, utilising JPEG2000 compression.

The extracting of the feature values, the embedding of the data corresponding to the feature values, and the creating of the image signature may be performed as part of the JPEG 2000 coding.

In accordance with a second aspect of the present invention there is provided a method of authenticating a digital image, the method comprising extracting feature values from the digital image based on a selected authentication bit-rate; and processing the extracted feature values to derive data corresponding to original feature values based on a selected authentication mode; and comparing the derived data corresponding to the original feature values with reference data derived from an image signature associated with the digital image.

Deriving the data corresponding to the feature values may comprise ECC coding the extracted data and extracted feature values.

The extracted feature values from each of a plurality of codeblocks of the digital image may be decoded to derive the data corresponding to the original feature values.

The method may further comprise extracting data embedded as a watermark in the digital image; and the processing the extracted data and the extracted feature values to derive the data corresponding to original feature values.

The method may further comprise applying ECC decoding twice to the extracted data.

The data may be embedded in a lossy or lossless way as a watermark in the digital image.

The method may further comprise applying a cryptographic technique to the image signature to derive a bit sequence representing the reference data.

The method may further comprise applying a public key to process the image signature for deriving the reference data.

The method may further comprise receiving the digital image as a coded digital image.

The digital image may be coded utilising JPEG2000.

The extracting of the data embedded as a watermark, the extracting of feature values from the digital image, the processing of the extracted data and extracted feature values, and the comparing of the derived data corresponding to the original feature values with the reference data may be performed as part of the JPEG 2000 de-coding.

In accordance with a third aspect of the present invention there is provided a system for protecting a digital image, the system comprising a feature value extractor device for extracting feature values from the digital image based on a selected authentication bit-rate; a mode selector for selecting an authentication mode for processing the extracted feature values; a processor device for deriving data corresponding to the extracted feature values based on the selected authentication mode; and wherein the processor device further creates an image signature based on the data corresponding to the feature values.

In accordance with a fourth aspect of the present invention there is provided a computer readable data storage medium having stored thereon computer program code means for instructing a computer to execute a method of protecting a digital image, the method comprising extracting feature values from the digital image based on a selected authentication bit-rate; selecting an authentication mode for processing the extracted feature values, the processing of the extracted feature values comprising deriving data corresponding to the extracted feature values based on the selected authentication mode; and creating an image signature based on the data corresponding to the feature values.

In accordance with a fifth aspect of the present invention there is provided a system for authenticating a digital image, the system comprising a feature value extractor device for extracting feature values from the digital image based on a selected authentication bit-rate; a processor device for processing the extracted feature values based on a selected authentication mode to derive data corresponding to original feature values and for comparing the derived data corresponding to the original feature values with reference data derived from an image signature associated with the digital image.

In accordance with a sixth aspect of the present invention there is provided a computer readable data storage medium having stored thereon computer program code means for instructing a computer to execute a method of authenticating a digital image, the method comprising extracting feature values from the digital image based on a selected authentication bit-rate; processing the extracted feature values based on a selected authentication mode to derive data corresponding to original feature values; and comparing the derived data corresponding to the original feature values with reference data derived from an image signature associated with the digital image.

BRIEF DESCRIPTION OF THE DRAWINGS

Embodiments of the invention will be better understood and readily apparent to one of ordinary skill in the art from the following written description, by way of example only, and in conjunction with the drawings, in which:

Figure 1 illustrates a prior art watermarking based authentication scheme.

Figure 2 shows signature based authentication scheme.

Figure 3 is a flow chart illustrating an image authentication process in accordance with an embodiment of the present invention.

Figure 4 is a schematic drawing illustrating signature signing and watermark embedding process flow in accordance with an embodiment of the present invention.

Figure 5 is a schematic drawing illustrating a watermark extracting and signature verification process flow in accordance with an embodiment of the present invention.

Figure 6 is a flowchart illustrating a method of protecting a digital image in an example embodiment.

Figure 7 is a flowchart illustrating a method of authenticating a digital image in an example embodiment.

CLAIMS

1. A method of protecting a digital image, the method comprising:

extracting feature values from the digital image based on a selected authentication bit-rate and a selected image content;

selecting an authentication mode for processing the extracted feature values, the processing of the extracted feature values comprising deriving data corresponding to the extracted feature values based on the selected authentication mode; and

creating an image signature based on the data corresponding to the feature values.

2. The method as claimed in claim 1, wherein the processing comprises correcting coding (ECC) the extracted feature values to derive the data corresponding to the feature values.

3. The method as claimed in claims 1 or 2, wherein the feature values from each of a plurality of codeblocks of the original digital image are thresholded and coded to create the data corresponding to the feature values.

4. The method as claimed in any one of claims 1 to 3, wherein the processing further comprises embedding the data corresponding to the feature values into the digital image.

5. The method as claimed in claim 2, further comprising applying ECC coding again to parity check bits generated during the ECC coding of the extracted feature values to generate the data corresponding to the feature values.

6. The method as claimed in claim 4, wherein the embedding of the data corresponding to the feature values as a watermark is conducted in a lossy or a lossless way, based on the selected authentication mode.

7. The method as claimed in any one of claims 1 to 6, wherein the creating of the image signature comprises applying a cryptographic hashing

function to a bit sequence representing the data corresponding to the feature values.

8. The method as claimed in any one of claims 1 to 7, wherein the creating of the image signature comprises utilising a private key.

9. The method as claimed in any one of claims 1 to 8, wherein the method further comprises distributing the digital image, including the embedded data, as the authentic digital image.

10. The method as claimed in any one of claims 1 to 9, further comprising coding the digital image, including the embedded data, utilising JPEG2000 compression.

11. The method as claimed in claim 10, wherein the extracting of the feature values, the embedding of the data corresponding to the feature values, and
the creating of the image signature are performed as part of the JPEG 2000 coding.

12. A method of authenticating a digital image, the method comprising:
extracting feature values from the digital image based on a selected authentication bit-rate; and
processing the extracted feature values to derive data corresponding to original feature values based on a selected authentication mode; and
comparing the derived data corresponding to the original feature values with reference data derived from an image signature associated with the digital image.

13. The method as claimed in claim 12, wherein deriving the data corresponding to the feature values comprises ECC coding the extracted data and extracted feature values.

14. The method as claimed in claims 12 or 13, wherein the extracted feature values from each of a plurality of codeblocks of the digital image are decoded to derive the data corresponding to the original feature values.

15. The method as claimed in any one of claims 12 to 14, further comprising extracting data embedded as a watermark in the digital image; and the processing the extracted data and the extracted feature values to derive the data corresponding to original feature values.

16. The method as claimed in claim 13, further comprising applying ECC decoding twice to the extracted data.

17. The method as claimed in claim 15, wherein the data is embedded in a lossy or lossless way as a watermark in the digital image.

18. The method as claimed in any one of claims 12 to 17, further comprising applying a cryptographic technique to the image signature to derive a bit sequence representing the reference data.

19. The method as claimed in any one of claims 12 to 18, further comprising applying a public key to process the image signature for deriving the reference data.

20. The method as claimed in any one of claims 12 to 19, wherein the method further comprises receiving the digital image as a coded digital image.

21. The method as claimed in claim 20, wherein the digital image is coded utilising JPEG2000.

22. The method as claimed in claim 22, wherein the extracting of the data embedded as a watermark, the extracting of feature values from the digital image, the processing of the extracted data and extracted feature values, and the comparing of the derived data corresponding to the original feature values with the reference data are performed as part of the JPEG 2000 de-coding.

23. A system for protecting a digital image, the system comprising:

a feature value extractor device for extracting feature values from the digital image based on a selected authentication bit-rate;

a mode selector for selecting an authentication mode for processing the extracted feature values;

a processor device for deriving data corresponding to the extracted feature values based on the selected authentication mode; and

wherein the processor device further creates an image signature based on the data corresponding to the feature values.

24. A computer readable data storage medium having stored thereon computer program code means for instructing a computer to execute a method of protecting a digital image, the method comprising:

extracting feature values from the digital image based on a selected authentication bit-rate;

selecting an authentication mode for processing the extracted feature values, the processing of the extracted feature values comprising deriving data corresponding to the extracted feature values based on the selected authentication mode; and

creating an image signature based on the data corresponding to the feature values.

25. A system for authenticating a digital image, the system comprising:

a feature value extractor device for extracting feature values from the digital image based on a selected authentication bit-rate;

a processor device for processing the extracted feature values based on a selected authentication mode to derive data corresponding to original feature values and for comparing the derived data corresponding to the original feature values with reference data derived from an image signature associated with the digital image.

26. A computer readable data storage medium having stored thereon computer program code means for instructing a computer to execute a method of authenticating a digital image, the method comprising:

extracting feature values from the digital image based on a selected authentication bit-rate;

processing the extracted feature values based on a selected authentication mode to derive data corresponding to original feature values; and

comparing the derived data corresponding to the original feature values with reference data derived from an image signature associated with the digital image.

20

METHOD AND SYSTEM FOR PROTECTING AND AUTHENTICATING A DIGITAL IMAGE

ABSTRACT

A method of protecting a digital image, the method comprising extracting feature values from the digital image based on a selected authentication bit-rate; embedding data corresponding to the feature values as a watermark in a into the digital image; and creating an image signature based on the data corresponding to the feature values.

FIG. 4